ISSUE BRIEF Global

NAVIGATING CROSS-BORDER DATA TRANSFERS IN THE APAC REGION

An Analysis of Developments from 2023 to 2026

July 2026 (Updated November 2026)

FUTURE OF PRIVACY FORUM

AUTHOR

Dominic Paulger, *Deputy Director for Asia Pacific*

EDITOR

Josh Lee Kok Thong, *Managing Director for Asia Pacific*

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

All FPF materials that are released publicly are free to share and adapt with appropriate attribution. Learn more at creativecommons.org.

Table of Contents

Executive Summary **4**

Introduction **5**

Background 5

An Overview of Key Developments in the APAC Region from 2023 to 2026 6

Trends in the APAC Region 8

Conclusion 10

Table 1. An overview of CBDT provisions in selected APAC jurisdictions (Updated July 2026) **11**

Appendix: Detailed Jurisdictional Updates **14**

Australia 14

China 15

South Asia 18

Bangladesh 18

India 20

Sri Lanka 22

Southeast Asia 24

Brunei Darussalam 24

Cambodia 25

Indonesia 25

Malaysia 28

Singapore 31

Thailand 31

Vietnam 32

Executive Summary

This Issue Brief examines the rapidly evolving landscape of cross-border data transfers (**CBDTs**) across the Asia-Pacific (**APAC**) region from 2023 to 2026. It updates a 2023 Issue Brief released by the Future of Privacy Forum (**FPF**), which covered 2021 to 2023.

It finds that while the core challenge for data protection laws in APAC remains balancing digital trade with protecting personal data, the frameworks governing this balance have shifted. This brief identifies six key trends in the changes that have taken place across the region from 2023 to 2026:

- APAC jurisdictions are increasingly **converging around safeguards-based mechanisms**, such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs).
- Adoption of "**whitelisting" mechanisms is expanding** in APAC, while certain APAC jurisdictions have adopted a **"blacklisting" approach**.
- Despite liberalization of requirements in some jurisdictions, **new restrictions on CBDTs** are emerging in others.
- There is a growing trend towards requiring organizations to conduct **Transfer Impact Assessments** (**TIAs**).
- **Regional frameworks and initiatives are gaining traction** to reduce fragmentation.
- Regulators are equipping themselves with **stronger enforcement tools**, raising the stakes for non-compliance with CBDT requirements.

The Appendix to this Issue Brief also offers detailed jurisdictional updates for Australia, China, South Asia (Bangladesh, India, Sri Lanka), and Southeast Asia (Brunei Darussalam, Cambodia, Indonesia, Malaysia, Singapore, Thailand, and Vietnam).

Introduction

In September 2023, the Future of Privacy Forum's (**FPF**)'s Asia-Pacific (**APAC**) office published an issue brief, "Navigating CBDTs in the Asia-Pacific Region," that summarized key developments in the regulation of cross-border data transfers (**CBDTs**) across the region between 2021 and 2023.

This Issue Brief serves as an update to the 2023 publication, analyzing the most significant developments in CBDTs across the APAC region in the three years since. It follows the structure of the original brief, providing a concise background, an updated analysis of regional trends, a comparative table of CBDT frameworks, and a detailed appendix of jurisdiction-specific developments. All specific details of bills, laws, provisions and other documents referred to in the concise background and the analysis of regional trends can be found in the country reports included in the appendix. For a comprehensive overview of the foundational transfer mechanisms discussed, readers are encouraged to refer to the original 2023 Issue Brief.

Background

CBDTs are the lifeblood of the global digital economy, enabling international trade, innovation, and communication. However, they also present risks to privacy and security. To mitigate these risks, data protection laws impose conditions on the transfer of personal data to other jurisdictions, aiming to ensure that the data remains adequately protected after it crosses a border.

As detailed in our 2023 Issue Brief, these conditions typically fall into several categories:

1. **Whitelisting or "Adequacy":** Permitting any transfers to specific jurisdictions that have been formally recognized as providing a comparable level of data protection.

2. **Appropriate safeguards:** Allowing transfers to any jurisdiction, regardless of its "adequacy" status, when the exporting organization implements specific measures to protect the data, most commonly through:

    a. **Legally binding agreements**, such as mandatory Standard Contractual Clauses (**SCCs**), or non-mandatory Model Contractual Clauses (**MCCs**);

    b. **Internal policies,** such as Binding Corporate Rules (**BCRs**); or

    c. **Certification schemes**, such as the APEC and Global Cross-Border Privacy Rules (**CBPR**) and Privacy Recognition for Processors (**PRP**) schemes.

3. **Consent:** Enabling transfers where the individual data subject has given their explicit and informed consent for a specific transfer.

4. **Necessity:** Permitting transfers in specific, exceptional circumstances, such as for the performance of a contract with the data subject, or to protect a person's vital interests.

Following developments in APAC since 2023, this Issue Brief adds a fifth category of conditions to the above list. Certain APAC jurisdictions, such as **India**, have adopted a "**blacklist**" approach: allowing transfers of personal data by default, with exceptions for transfers to certain jurisdictions or concerning certain kinds of information.

Jurisdictions often arrange these mechanisms in a hierarchy, prioritizing adequacy and safeguards over consent and other exceptions. The specific combination and implementation of these mechanisms vary significantly across the APAC region, reflecting diverse policy priorities.

An Overview of Key Developments in the APAC Region from 2023 to 2026

Since 2023, the legal and regulatory landscape in the APAC region has continued to evolve rapidly. The core challenge for organizations – balancing the immense economic benefits of digital trade with the imperative to protect personal data – remains; however, the frameworks governing this balance have shifted significantly.

The region has seen the emergence of several new data protection laws.

- In August 2023, **India** enacted its first comprehensive data protection law, the Digital Personal Data Protection Act, 2023 (**DPDPA**), establishing a liberal "blacklist" model – transfers to territories outside of India are permitted by default, but the Government reserves the power to restrict transfers to specific territories.

- In 2025, **Vietnam** enacted a new data protection law, replacing its previous decree with a new Law on Personal Data Protection. This new Law retains but expands upon the former Decree's TIA-based approach to governing CBDTs.

- In March 2025**, Brunei Darussalam** enacted its first comprehensive data protection law, closely mirroring Singapore's framework, including for CBDTs.

- Most recently, **Cambodia** began consultations on a draft data protection law that adopts a GDPR-style approach to CBDTs, and **Bangladesh** enacted its first comprehensive data protection law.

Several jurisdictions have amended the cross-border data transfer aspects of their data protection laws.

- In October 2024, **Malaysia** amended its Personal Data Protection Act, replacing an unused government-managed "whitelist" system with new provisions allowing controllers to determine if the destination country provides a level of data protection that is "substantially similar" or offers an "equivalent level of protection" to Malaysia's PDPA. In April 2025, the country's Personal Data Protection Department (**PDPD**) followed up with new guidelines to facilitate compliance with these new provisions, and in November 2026, Malaysia was accepted as a full member of the APEC CBPR System.

- In December 2024, **Australia** amended its Privacy Act to formally introduce a "whitelist" mechanism, allowing the government to officially recognize countries and binding schemes with "substantially similar" data protection laws, thereby streamlining data flows to trusted destinations.

Jurisdictions, especially those with newer data protection laws, have also taken steps to operationalize cross-border data transfer rules (among other aspects) of these laws through subordinate regulations.

- In March 2024, **Thailand**'s Personal Data Protection Committee (**PDPC**) put into effect two key regulations on CBDTs, operationalizing key provisions of the country's PDPA. These long-awaited regulations clarify the use of adequacy, BCRs, and SCCs, providing much-needed certainty for businesses. Notably, they also recognize the ASEAN MCCs and EU SCCs as valid transfer tools.

- In November 2025, **India**'s Ministry of Electronics and Information Technology (**MEITY**) released implementing regulations for the DPDPA, the Digital Personal Data Protection Rules, 2025 (**DPDP Rules**). Whereas an earlier draft of the DPDP Rules, released for public consultation in January 2025, appeared to introduce new restrictions on cross-border data transfers, the final version repeated the DPDPA's "blacklist" approach, clarifying that any personal data processed under the DPDPA may be transferred out of India, subject only to requirements specified by the Central Government via general or special order.

While the CBDT provisions of **Sri Lanka**'s Personal Data Protection Act, No. 9 of 2022 (**PDPA**) will only take effect from January 2027, the country's Data Protection Authority (**DPA**) has already released a detailed draft directive that outlines a range of mechanisms for complying with the PDPA's CBDT requirements.

Implementing regulations for **Indonesia**'s Personal Data Protection Law (**PDPL**) were released publicly in July 2026 – two years after the PDPL became enforceable in October 2024. The implementing regulations provide important operational details for the PDPL's three transfer mechanisms (adequacy, equivalent or high protection, and consent) and introduce new requirements to notify data subjects of the transfer, and conduct a transfer impact assessment (**TIA**).

China has sought to liberalize its CBDT regulations and facilitate transfers with Special Administrative Regions (**SARs**) Hong Kong and Macau.

- The March 2024 **Regulations on Promoting and Standardising Cross-Border Data Flows** created crucial exemptions from the three primary transfer mechanisms (security assessment, SCCs, and certification) for routine business activities, such as performing contracts, managing human resources, and for low-volume transfers.

- Simultaneously, China has pioneered a "negative list" approach within its Pilot Free Trade Zones (**FTZs**). In zones like Tianjin, Beijing, and Shanghai, data not explicitly included on a negative list is presumed to be exempt from formal transfer compliance procedures. This creates a dynamic of "competitive federalism," where FTZs can offer more liberal data transfer regimes to attract investment in specific industries. A parallel development in the Guangdong-Hong Kong-Macao

Greater Bay Area (**GBA**) introduced a bespoke Standard Contract, streamlining data flows within this critical economic zone under the condition that the data remains localized within the GBA.

ASEAN's efforts to foster regional interoperability continue.

- At the regional level, initiatives to foster interoperability also continue to mature, with the Association of Southeast Asian Nations (**ASEAN**) publishing guidelines comparing the ASEAN MCCs with the European Union (**EU**)'s SCCs and Ibero-American Data Protection Network's MCCs.

- ASEAN Member States also concluded negotiations on a landmark Digital Economy Framework Agreement (**DEFA**) in late May 2026. The DEFA, which specifically addresses CBDTs, is targeted to be signed at the 49th ASEAN Summit, to be held from 16 to 18 November 2026 in Manila, in the Philippines.

Trends in the APAC Region

Building on the trends identified in the 2023 Issue Brief, this review of recent developments in cross-border transfers in the APAC region reveals a region that is becoming more complex. A greater number of jurisdictions now have comprehensive data protection laws in place. However, there are still significant variations in their approaches to cross-border transfers, reflecting governments' efforts to balance economic integration, national security, and data privacy.

While the underlying principles often draw from global benchmarks, the diversity of legal, political, and economic contexts has produced varied – and sometimes competing – models. Several notable trends can be identified:

1. APAC jurisdictions are increasingly converging around safeguards-based mechanisms.

Jurisdictions across the region are increasingly adopting safeguards-based mechanisms (that is, specific mechanisms or measures that can be implemented by an exporting organization to protect the data being transferred) as the foundation of CBDT regimes. These include:

- Standardized contractual language, such as non-mandatory MCCs and mandatory SCCs;

- BCRs; and

- Certification schemes, such as the APEC and Global CBPRs.

Between 2023 and 2026, Australia, Malaysia, Thailand, and Sri Lanka have all sought to provide greater legal certainty around the use of such mechanisms. These mechanisms provide organizations with contractual and organizational tools to mitigate risks and align with global best practices. The trend underscores a move away from rigid, one-size-fits-all prohibitions and "consent"-as-exception models as anchors of CBDTs, toward flexible compliance instruments that allow businesses to operationalize transfers within defined legal boundaries.

2. Adoption of whitelisting mechanisms is expanding in APAC, while certain APAC jurisdictions have adopted a "blacklisting" approach.

Many jurisdictions in APAC are adopting whitelist-style frameworks, under which transfers are permitted to other jurisdictions that are deemed to provide "substantially similar" protection to that provided by domestic data protection law.

Australia has recently implemented a mechanism akin to the EU's adequacy decisions, while **Malaysia**'s amendments to the PDPA now allow transfers to jurisdictions assessed by controllers as substantially similar.

By contrast, **India's** DPDPA and DPDP Rules establish a fairly liberal "blacklist" model, permitting transfers to all countries unless specifically restricted.

China's FTZs and the Guangdong-Hong Kong-Macao GBA have experimented with tailored whitelist and negative-list models, reflecting an interest in regulated liberalization. These approaches aim to facilitate trusted flows with strategic partners while maintaining national oversight.

3. Restrictions on CBDTs are re-emerging in APAC.

Despite the rise of safeguards and adequacy models, several jurisdictions continue to impose or reintroduce restrictions on CBDTs, especially for sensitive or strategically important data. Implementing rules for India's new data protection law introduce new layers of discretionary control over data transfers and new localization mandates, while **Vietnam**'s new Data Law and draft Data Security Law establish strict requirements for "core" and "important" data. These obligations reflect security-driven policy priorities, often tied to concerns over foreign access, financial stability, or national sovereignty. The result is a **dual-track environment**: more liberalized transfers for general data, alongside stringent controls for data deemed critical.

4. There is a growing trend in APAC towards requiring transfer impact assessments.

Several regimes now place greater responsibility on organizations to evaluate the risks of overseas transfers. **Indonesia**, **Malaysia**, **Sri Lanka**, **Thailand,** and **Vietnam** have all issued requirements around the use of TIAs or equivalent due diligence processes. These assessments require organizations to examine both the legal protections in the recipient jurisdiction and the practical enforceability of safeguards. The shift reflects a growing emphasis on accountability and organizational responsibility.

5. Regional frameworks and Interoperability Initiatives are gaining traction in APAC.

Regional cooperation is gaining traction as economies seek to reduce compliance fragmentation and enable trusted data flows within blocs. ASEAN's joint guidance with the EU and Ibero-American Network, and the forthcoming DEFA, with dedicated provisions on cross-border data transfers, highlight this momentum. Similarly, **China**'s Greater Bay Area Standard Contract introduces a localized "data bubble,"

while the APEC and Global CBPR initiatives continue to expand recognition frameworks. These efforts point to a future of layered interoperability, where businesses may rely on regional frameworks to supplement national regimes.

6. Enforcement is on the rise in APAC, and the stakes for non-compliance are higher.

Finally, regulators are increasingly equipping themselves with stronger enforcement tools. **Vietnam**'s new PDP Law and the implementing regulations for **Indonesia's** PDPL introduce revenue-based fines, while **Brunei** and **Malaysia**'s amended frameworks provide for substantial financial penalties. This trend signals a shift from aspirational standards to hard enforcement, compelling organizations to prioritize CBDT compliance as part of broader data governance strategies.

Conclusion

Taken together, these trends illustrate a **dual dynamic**: **convergence toward international safeguards and accountability standards, alongside divergence in localization and sovereignty-driven measures**. For multinational organizations, this means navigating a patchwork of overlapping regimes, with rising compliance costs and strategic decisions about data infrastructure. At the same time, regional frameworks promise incremental relief by offering pathways to interoperability and predictability. Businesses operating across the APAC region must therefore balance local compliance with regional alignment, while preparing for a future where cross-border data governance is simultaneously globalizing and fragmenting.

Table 1. An overview of CBDT provisions in selected APAC jurisdictions (Updated November 2026)

	Australia	China	Bangladesh	India	Indonesia	Malaysia	Sri Lanka	Thailand	Vietnam
Adequacy / Whitelist	**Yes.** The Government may prescribe countries but has not done so to date.	**No**.	**No.** However, the destination must have "appropriate technology and equipment," as defined by future regulations.	**No**. "Blacklist" model: personal data may be transferred out of India, subject to restrictions ordered by the Central Government.	**Yes**. Indonesia's DPA (not yet established) may issue adequacy decisions but has not done so to date.	**No**. However, controllers may assess whether the destination's law is "substantially similar."	**Yes**.	**Yes**. The PDPC can issue adequacy decisions but has not done so to date.	**No**.
Certification	**Yes.** The Government may prescribe schemes but has not done so to date.	**Yes**.	**No.**	**Possible**. Certifications are not required but could optionally be adopted.	**Possible.** The implementing regulations for the PDPL do not expressly reference certifications but allow for the DPA to recognize "adequate and binding" instruments.	**Yes**. New CBDT Guidelines clarify that certifications can be relied on under existing provisions of the PDPA. Malaysia became a full member of the APEC CBPR System in November 2026	**Yes**.	**Yes**.	**No**.

	Australia	China	Bangladesh	India	Indonesia	Malaysia	Sri Lanka	Thailand	Vietnam
Standard Contractual Clauses (SCCs) / Binding Agreements	**Possible.** However, no official SCCs have been released.	**Yes.** SCCs are mandatory for most transfers not requiring security assessment.	**Yes.**	**Possible**. SCCs are not required but could optionally be adopted. No official SCCs have been released.	**Yes.** Indonesia's DPA (not yet established) is empowered to prescribe SCCs.	**Yes**. New CBDT Guidelines clarify that contractual clauses can be relied on under existing provisions of the PDPA.	**Yes**.	**Yes**. Regulations recognize ASEAN MCCs and EU SCCs.	**No**.
Binding Corporate Rules (BCRs)	**Possible.** However, there are no specific provisions on this.	**No**. Certification is the main mechanism for intra-group transfers.	**No.**	**Possible**. BCRs are not required but could optionally be adopted.	**Yes.** Indonesia's DPA (not yet established) is empowered to prescribe BCRs.	**Yes**. New CBDT Guidelines clarify that BCRs can be relied on under existing provisions of the PDPA.	**Yes**.	**Yes**. BCRs must be certified by the PDPC.	**No**.
Consent	**Yes**.	**No**. However, consent may still be required.	**Yes.**	**No**. However, consent may still be required.	**Yes.**	**Yes**.	**Yes**.	**Yes**.	**No**. However, consent may still be required.

	Australia	China	Bangladesh	India	Indonesia	Malaysia	Sri Lanka	Thailand	Vietnam
Mandatory Filing / Govt. Approval	**No.**	**Yes.**	**Yes.** Certain transfers of personal data must be notified.	**No.** However, the Government can impose restrictions on cross-border data transfers to certain territories or concerning certain kinds of personal data	**No.**	**No.**	**No.**	**No.**	**Yes.** A Data Transfer Assessment must be filed with the Ministry of Public Security. Stricter notification and approval requirements apply to Important and Core Data.

Appendix: Detailed Jurisdictional Updates

Australia

Privacy and Other Legislation Amendment Bill 2024

Since 2023, Australia has seen significant legal developments concerning its privacy framework, particularly regarding cross-border data transfers, stemming from a **multi-year public consultation** on updating the Privacy Act of 1988 (**Act**) led by the Attorney-General's Department (**AGD**).

- In February 2023, following extensive public consultation, the AGD released its **Privacy Act Review Report**. The Report contained 116 proposals to reform the Act across 28 key areas.

- In September 2023, the Australian Government published its **Response** to the AGD's report, agreeing in-principle to introduce a mechanism to "prescribe countries with substantially similar privacy laws" to the Act. The Government also agreed to the development of standard contractual clauses for data transfers to non-prescribed countries.

- A year later, in September 2024, the Australian Government tabled the "**Privacy and Other Legislation Amendment Bill 2024**" (**Bill**). The Bill, among other provisions, introduced a new mechanism enabling entities to transfer personal information to other countries, or according to binding schemes, that have been prescribed in regulations as providing "substantially similar" privacy protections to the Act. The Bill was passed in November 2024 and took effect in December 2024.

These 2024 amendments introduced new provisions to **Australian Privacy Principle (APP) 8**, which governs the cross-border disclosure of personal information under the Act.

By default, APP 8 requires an APP Entity that intends to disclose personal information to an overseas recipient to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to that information. This default rule is subject to several exceptions, including informed consent, and necessity for several important purposes, such as law enforcement and responding to health emergencies.

The 2024 amendments expand these exceptions by establishing a new whitelisting mechanism that allows transfers of personal information if the recipient is:

- subject to the laws of a country; or

- a participant in a binding scheme,

that is prescribed by regulations, after the Governor-General of Australia determines that the country or scheme provides **"substantially similar" protection to the APPs** and has enforcement mechanisms that are available to individuals. This whitelisting can also be made subject to specific conditions for certain entities or types of personal information.

These new provisions complement existing provisions of the Act that allow cross-border data transfers if an entity *reasonably believes* that the recipient is subject to a law or binding scheme that provides substantially similar protection to the APPs, and there are mechanisms available for individuals to enforce that protection.

The Explanatory Memorandum to the Bill clarifies that "substantially similar" means a comparable or higher level of privacy protection provided by the APPs, with the overall effect of the law or scheme being considered, rather than a direct correspondence of each provision.

These amendments, if fully implemented, could potentially simplify compliance with APP 8 by pre-approving transfers to jurisdictions deemed "adequate" or offering "substantially similar" protection, rather than requiring entities to individually assess the situation of every recipient. They also create possibilities for the Australian Government to approve other common transfer mechanisms, such as certifications and BCRs, under this provision in the future.

China

Since 2023, China has significantly evolved its data governance framework, introducing new regulations and mechanisms that directly impact the cross-border transfer of personal information. These developments aim to balance the promotion of data flows with national security and individual privacy, creating a complex but increasingly structured environment for businesses.

1. Regulations on Promoting and Standardizing Cross-Border Data Flows

The Cyberspace Authority of China (**CAC**)'s **Regulations on Promoting and Standardising Cross-Border Data Flows** (**CBDF Regulations**), which took effect on 22 March 2024, represent a significant step in clarifying China's CBDT rules. These regulations modify the application of the Personal Information Protection Law (**PIPL**), particularly concerning when a security assessment by the CAC is required, and when certain data transfers are exempt from the standard PIPL mechanisms.

Clarifications on CAC Security Assessment Requirements

A security assessment by the CAC is required for transfers involving:

- "Important data".
- Personal information of over 1 million individuals.
- Sensitive personal information of over 10,000 individuals.
- Any personal information transfer by critical information infrastructure operators (CIIOs).

Exemptions from PIPL Transfer Mechanisms

The CBDF Regulations introduce exceptions from the requirement to use one of the PIPL's three mechanisms for transferring personal information out of China (i.e., data export security assessments, concluding standard personal information export contracts, and passing personal information protection certification).

These exceptions cover:

- **Data collected or produced in specific international activities**, such as international trade, cross-border transport, academic cooperation, and multinational manufacturing and marketing, provided that the data does not include personal information or important data.

- **Re-exports of personal information that was collected or produced by data handlers overseas** but transmitted to China for handling, provided that no domestic personal information or important data was introduced during the handling.

- **Specific transfers of personal information** (provided this does not include important data) that are genuinely necessary for:

    - **Concluding or performing contracts** to which an individual is a party (e.g., cross-border purchases, plane/hotel reservations, visa handling, cross-border payments);

    - **Cross-border human resource management** for employees, in accordance with lawfully formulated labour rules and collective contracts;

    - **Emergencies** to protect the lives and wellbeing of natural persons, and the security of their property;

    - Data handlers (other than CIIOs) who have **cumulatively transferred less than 100,000 persons' personal information** (not including sensitive personal information) overseas before 1 January of that year.

Free Trade Zone (FTZ) "Negative Lists"

A unique aspect of the CBDF Regulations is the empowerment of China's "Pilot Free Trade Zones" (**FTZs**) to create their own exemptions, known as "negative lists."

This approach fundamentally inverts the default posture of Chinese data law – for eligible companies registered within a designated FTZ, any data not explicitly enumerated on the zone's negative list is presumed to be exempt from the PIPL's compliance procedures for cross-border data transfers. This contrasts with the national model, which assumes all data transfers require a formal compliance mechanism unless specifically exempted.

To date, 9 FTZs (Tianjin, Zhejiang, Jiangsu, Guangxi, Chongqing, Fujian, Shanghai, Beijing, and Guangdong) and the Hainan Free Trade Port have established and filed their respective data export management lists, which vary significantly in scope and industry focus.

It is important to note that while these FTZ negative lists provide exemptions from the formal cross-border data transfer procedural mechanisms, they are not a blanket waiver of other data protection obligations under the PIPL, such as having a legal basis for processing personal information.

2. Initiatives to Promote Cross-Border Data Transfers within the Guangdong-Hong Kong-Macao Greater Bay Area (GBA)

The **Guangdong-Hong Kong-Macao Greater Bay Area** (**GBA**) is a key strategic region spanning China's southern Guangdong province (home of technology hub Shenzhen), as well as the country's two Special Administrative Regions (**SARs**), Hong Kong, and Macao. The GBA has seen significant efforts to facilitate cross-boundary data flows and address the challenges posed by the "One Country, Two Systems" policy, which have resulted in the mainland and the SARs adopting fundamentally different legal regimes for data protection and security.

This initiative began with a "**Memorandum of Understanding on Facilitating Cross-boundary Data Flow within the Guangdong-Hong Kong-Macao Greater Bay Area**" (**MoU**), which Cyberspace Administration of China (**CAC**) and Hong Kong's Innovation, Technology & Industry Bureau (**ITIB**) entered into in June 2023. This MoU established a political consensus to create bespoke security rules for GBA data flows, aiming for safe and orderly data movement to promote the GBA's high-quality development.

The first major milestone in the initiative came six months later, in December 2023, with the release of a **Standard Contract for the GBA** (**GBA SC**) and accompanying **Implementation Guidelines**. The GBA SC is a bespoke legal instrument designed to create a streamlined, predictable, and officially sanctioned channel for personal information flows within the GBA.

The GBA SC applies exclusively to cross-boundary transfers of personal information between the Hong Kong SAR and the nine designated cities in Guangdong Province (Guangzhou, Shenzhen, Zhuhai, Foshan, Huizhou, Dongguan, Zhongshan, Jiangmen, and Zhaoqing). Macao is conspicuously absent. Both the data exporter ("Personal Information Processor") and the data importer ("Recipient") must be either registered as an organization, or physically located as an individual, within this prescribed territory.

This, in effect, creates a regulated "data bubble" around the GBA, offering a reduced compliance burden (such as the removal of data volume caps, and a less onerous impact assessment) in exchange for a strict requirement that the data must remain within the bubble permanently. Personal information transferred using the GBA SC cannot be subsequently provided or made accessible to any organization or individual located outside the defined GBA territory. This includes transfers to other entities within the same corporate group outside the GBA and prevents remote access to the data from systems or personnel located outside the GBA

The GBA SC also explicitly does not apply to the transfer of "important data." However, the GBA Implementation Guidelines clarify that companies may presume that their data is non-important, unless

they have been explicitly notified otherwise by a regulatory authority, or if the data falls into a publicly announced catalogue of important data.

South Asia

Bangladesh

On 10 April 2026, the Government of Bangladesh enacted the **Personal Data Protection Act, 2026 (Act No. 63 of 2026)** (**Act**).

The Act repeals the country's first comprehensive data protection instrument, the **Personal Data Protection Ordinance, 2025 (Ordinance No. 61 of 2025)**, enacted in November 2025, as well as the **Personal Data Protection (Amendment) Ordinance, 2026 (Ordinance No. 23 of 2026)**, enacted in February 2026. However, the provisions of the Act are very similar to those of the earlier Ordinances.

Most provisions of the Act were deemed to have taken effect from 6 November 2025. Provisions on the appointment of chief data officers (Section 23), and the Act's enforcement and penalty framework (Sections 31 to 35), will take effect 18 months from the promulgation of the Act, on a date to be notified by the Government in the Official Gazette.

Transfers of personal data

Under the Act, a Data Fiduciary – broadly, an entity that determines the purpose for processing personal data – must pass a two-step test to lawfully transfer personal data out of Bangladesh under the Act.

First, the Data Fiduciary must satisfy the requirements for one of the three transfer mechanisms in **Section 29(3)** of the Act, namely:

- **Consent** of the data subject concerned;
- **Contractual necessity** – that is, the transfer involves the exchange of goods or services under a contract to which the data subject is a party; or
- **Interests of the data subject, with the data subject's consent.** For this mechanism, the transfer should involve the data subject's interests regarding business, education, exit, or immigration, and the data subject consents to the transfer. However, in practical terms, it is unclear how this provision differs from the default consent provision above.

Second, the Data Fiduciary must also comply with **Section 29(4)** of the Act, which requires that personal data may only be transferred to locations or countries where "appropriate technology and equipment exist for the preservation of personal data." The criteria for determining whether this requirement is met will be provided in forthcoming regulations.

However, certain transfers are subject to more stringent requirements.

Transfer of "Sensitive Personally Identifiable Information"

In addition to the requirements of Section 29(3) of the Act, **Section 29(6)** requires Data Fiduciaries to notify the Authority if they transfer "massive amounts" of "**sensitive personally identifiable information**" across borders. Section 29(6) defines the latter term to mean:

- **Government-issued unique identification numbers**, such as national identity card numbers, passport numbers, tax identification numbers, and permanent account numbers;
- **Biometric identifiers**, such as fingerprints, facial recognition information, and iris scans;
- **Genetic, or DNA-related information;** and
- **Information relating to criminal records or sentencing,**

that, if transferred in "massive amounts," may create a risk to Bangladesh's state sovereignty, national security, or financial stability. The Act does not specify any thresholds for the phrase "massive amounts" (বিপুল পরিমাণ). The term "**sensitive personally identifiable information**" also appears to be distinct from "**sensitive personal data**" which is defined in Section 2(21) of the Act, and is broader in scope.

Removal, but potential return, of data residency

Previously, Ordinance No. 61 of 2025 and its subsequent amendment (Ordinance No. 23 of 2026) imposed stringent requirements on CBDTs to cloud computing infrastructure. These included mandates to maintain a "synchronized real-time copy" of restricted personal data within Bangladesh, provide a "data dictionary" to the National Data Management Authority, and comply with strict infrastructure migration orders.

The Act removes these data residency and local mirroring requirements. However, Section 29(1) of the Act retains the previous Ordinances' data classification framework. This framework, which applies solely to the Act's CBDT provisions in Section 29, empowers Bangladesh's National Data Management Authority (**Authority**) to classify personal data into four distinct classes. These are defined in the **Schedule** to the Act as follows:

- **Public or open personal data:** Any personal data that is made legally accessible to the public through a government publication, open platform, registry or similar legal means, or by the data subject. This category includes personal data that is intentionally disclosed for the public interest, provision of public services, research, or government transparency, and where there is no reasonable risk of harm if the data is processed responsibly.
- **Internal personal data**: Any non-publicly available personal data that is processed and stored for the legitimate internal operations of an organization or entity for operational, administrative, human resources, or customer service purposes. This category includes "non-sensitive personal data" such as employment details, contact details, or service usage history, and may also include sensitive personal data if processed in an internal context and under strict safeguards prescribed by law.

- **Confidential personal data**: Any personal data, including any sensitive personal data as defined in the Act, which, if disclosed, shared or processed without adequate safeguards, could result in significant harm, discrimination or breach of privacy to the data subject. This includes financial, health, biometric and real-time location data, as well as any data deemed sensitive or confidential by law or regulation that can be used to specifically identify an individual.

- **Restricted personal data**: Any personal data which has a potential impact on national security, public order, defence, critical infrastructure, or the fundamental rights and freedoms of an individual and which is subject to the strictest controls when processed, transferred or accessed. This category may also include classified datasets, sensitive health or security-related data, or any other personal data identified as "restricted" by the authorities or government.

Currently, the Act subjects all four categories to the exact same requirements for CBDTs (see above). However, considering the similarities between the Act and the earlier Ordinances, it is possible that new, category-specific data residency requirements – echoing those found in the repealed Ordinances – could be reintroduced in the future. These requirements may be established through regulations issued by the Authority under Section 29(7) of the Act, or through future legislative amendments.

Fee for transferring personal data

Section 29(6) of the Act empowers the Government of Bangladesh to prescribe a fee or charge on the annual business or commercial profits of any organization arising out of the use of personal data of Bangladeshi citizens.

Penalties

Chapter VIII of the Act (not yet in force) outlines penalties for infringing data subjects' rights under the Act (Section 32) and for failing to provide adequate protection and security of personal data as required by the Act (Section 33).

Neither of the penalty provisions expressly reference CBDTs, so it is uncertain whether breach of Section 29 of the Act would fall under Section 32 or Section 33. Both provisions are subject to an **administrative fine** of up to BDT 2.5 million (25 lakh, or approximately USD 20,310). However, Section 32 doubles the fine for Significant Data Fiduciaries, and additional fines for repeat violations.

India

Since 2023, India has undergone significant legal developments concerning personal data protection, most notably with the enactment of the **Digital Personal Data Protection Act, 2023** (**DPDPA**), and the subsequent release of implementing regulations for the DPDPA, the **Digital Personal Data Protection Rules, 2025** (**DPDP Rules**) in November 2025.

1. Digital Personal Data Protection Act 2023

The DPDPA establishes India's first cross-sectoral legal framework for personal data protection. It was approved by India's Cabinet on 5 July 2023 and received Presidential assent on 11 August 2023. The

DPDPA will come into effect in stages, according to timelines stated in a notification from the Ministry of Electronics and Information Technology (**MEITY**). The DPDPA's provisions on cross-border data transfers take effect on **13 May 2027** (eighteen months from date that the notification was issued (i.e., 13 November 2025).

The cornerstone of the DPDPA's cross-border transfer regime is found in **Section 16**, which enables Data Fiduciaries (the entities determining the purpose and means of processing personal data) to transfer personal data for processing to any country or territory outside India. Section 16 imposes only one explicit limitation: the Central Government may, through notification, **restrict the transfer of personal data to certain specified countries or territories**. This "blacklist" model permits all transfers by default, unless a specific destination is explicitly prohibited, contrasting with the "whitelist" approach of the EU's GDPR, and several jurisdictions in the APAC region.

However, a crucial, and often overlooked, provision is **Section 16(2)** of the DPDPA, which clarifies that nothing in the DPDPA restricts the applicability of any other Indian law that provides for a "higher degree of protection for, or restriction on, the transfer of personal data outside India."

This effectively establishes a **dual-track system**: a seemingly liberal "blacklist" for the general digital economy, alongside potentially more stringent rules for specific sectors.

An example of sectoral regulation imposing more stringent CBDT rules than those in the DPDPA is the **Reserve Bank of India's (RBI) directive on Storage of Payment System Data (April 2018)**, which mandates that all licensed payment system operators store all data relating to payment transactions exclusively within India. While processing abroad is allowed, data must be brought back to India and stored locally within 24 hours or one business day, and the copy stored abroad must be deleted.

2. Digital Personal Data Protection Rules, 2025

The DPDP Rules serve as implementing regulations for the DPDPA. MEITY published an initial draft of the Rules on 3 January 2025 for a public consultation until 18 February 2025 – this period was subsequently extended until 5 March 2025 MEITY subsequently notified the final version of the Rules on 13 November 2025.

Rule 15, which governs transfers of personal data out of India, closely mirrors Section 16 of the DPDPA, setting the framework for permitted transfers, subject to conditions specified by the Government. Rule 15 clarifies that the Data Fiduciary must "meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State."

However, the general provision in Rule 15 is subject to a significant exception – **Rule 13(4)** – which applies *only* to Significant Data Fiduciaries (**SDFs**). Rule 13(4) requires an SDF to undertake measures to ensure that certain personal data is processed "subject to the restriction that the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India." It also clarifies that personal data subject to this restriction will be specified by the Central Government on the recommendation of a dedicated committee.

The most direct implication of this provision is that it enables the Indian Government to establish **data localization** or **data residency requirements** for certain categories of data handled by SDFs. Notably, Rule 13(4) is comprehensive in scope, requiring that the restriction applies not only to the specified personal data but also to the "traffic" data pertaining to its flow. This means SDFs must ensure that metadata associated with the transmission and routing of specified personal data remains within India. However, the scope of localization is not static and can be dynamically adjusted based on evolving assessments of risk and sensitivity by the Central Government and its advisory committee.

Sri Lanka

1. Personal Data Protection Act

While Sri Lanka's Data Protection Authority (**DPA**) has been established and is active, Sri Lanka's **Personal Data Protection Act, No. 9 of 2022** (**PDPA**) has yet to take effect.

The original enforcement date for the core provisions of the PDPA – Part III (which includes CBDT requirements in Section 26) – was 18 March 2025, but this was repealed by **Extraordinary Gazette No. 2427/34**, leaving these provisions in a state of suspended animation. The **Personal Data Protection (Amendment) Act, No. 22 of 2025**, enacted in October 2025, empowered the Government to appoint a date for the commencement of the suspended core provisions of the PDPA.[1] On 22 July 2026, the Government issued **Extraordinary Gazette No. 2498/16**, which appointed **1 January 2027** as the effective date for Part III (together with several other core provisions) of the PDPA.

Section 26 of the PDPA recognizes multiple legal bases for transferring personal data out of Sri Lanka. These include:

- **Adequacy decisions** to be made by the Government of Sri Lanka on the advice of the DPA;
- **Appropriate safeguards:** Controllers and processors may adopt instruments specified by the DPA which subject the recipient of the data to "binding and enforceable commitments" to ensure appropriate safeguards to the rights of the data subjects and remedies protected by the PDPA.
- **Consent:** The data subject must explicitly consent to the processing of their personal data outside Sri Lanka, after having been informed of the possible risks of such processing for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- **Necessity** for:
    - Performance of a contract between the data subject and the controller, or the implementation of any pre-contractual measures taken by the controller at the request of the data subject;
    - Establishment, exercise, or defence of legal claims relating to the data subject;

[1] For an overview of the 2025 Amendments and the state of play, see Jayantha Fernando, "Data Privacy Legislation in Sri Lanka and Alignment with Global Standards", Eurolink, June 2026, p. 28.

- Public interest as defined in the PDPA; or
- Responding to an emergency that threatens the life, health, or safety of the data subject or another person, where the data subject or their legal guardian is physically or legally incapable of giving consent;

- **Permission under any conditions prescribed under the PDPA.**

2. Draft Guidelines on CBDTs

Sri Lanka's DPA has signaled its intended approach to implementing Section 26 of the PDPA by publishing a **"Draft Directive on Specification of Instruments for Processing Personal Data Outside Sri Lanka"** for public consultation in late 2024.

The draft directive outlines the specific mechanisms that non-public authorities can adopt to satisfy the "appropriate safeguards" requirement for transferring personal data outside Sri Lanka. These include:

- BCRs;
- Legal agreements that impose "binding and enforceable" data protection obligations on the recipient;
- Codes of conduct; and
- Certification schemes.

The draft directive also introduces novel governance requirements that are not present in the PDPA. These include:

- Conducting a **Cross-Border Processing Impact Assessment (CBPIA)** focusing on the legal framework and enforcement mechanisms in the third country, as well as the specific binding commitments of the recipient; and
- For specific scenarios, ensuring that the transferring entity's **board of directors** (or equivalent authority) pass a **resolution** ensuring that all necessary steps will be taken to comply with the PDPA's obligations.

The future of the draft directive remains uncertain, pending the amendments to the PDPA. For instance, if the amendments introduce changes to Section 26 of the PDPA or other related provisions, the draft directive would likely need to be revised or reissued to align with the new statutory requirements.

Southeast Asia

Brunei Darussalam

Brunei enacted its first comprehensive data protection law, the **Personal Data Protection Order, 2025** (**PDPO**), on 6 March 2025. The law, which took effect on 1 January 2026, is closely modeled on Singapore's PDPA.

Brunei's Authority for Info-communications Technology Industry (AITI) is responsible for administering the PDPO, with powers to impose penalties of up to BND 1 million (approximately USD 752,000) or 10% of the offending organization's annual turnover in Brunei if it exceeds BND 10 million (approximately USD 7.5 million)**.**

Section 24 of the PDPO specifically governs the transfer of personal data outside of Brunei Darussalam. This provision is near-identical to Section 26 of Singapore's PDPA and outlines two main options for cross-border data transfers**:**

Compliance with Forthcoming Implementing Regulations

This option requires organizations to comply with forthcoming implementing regulations to the PDPO that will specify to ensure that personal data transferred is protected to a comparable standard of protection to that under the PDPO.

As these regulations have not yet been enacted, this option is not currently available. However, given the PDPO's close similarities to Singapore's PDPA, it is possible that these implementing regulations will follow the example of **Part 3 of** **Singapore's Personal Data Protection Regulations 2021**, which provide for mechanisms such as:

- Consent from the data subject;
- Necessity for a range of different purposes under the PDPA;
- Legally binding obligations (e.g., through contracts, or BCRs);
- Certifications under approved schemes.

Application for Exemption to the AITI

The second option allows organizations to submit an application to the AITI for an exemption from the requirements outlined above. The PDPO provides that such an exemption may be granted either in full or subject to specific conditions.

Cambodia

Cambodia is in the process of establishing its first comprehensive data protection law. On 31 July 2026, Cambodia's Ministry of Post and Telecommunications (**MPTC**) released an updated draft of the **Law on Personal Data Protection** (**Law**) for public consultation.

The draft Law largely mirrors the structure of the EU's General Data Protection Regulation (**GDPR**), adopting GDPR-style data processing principles, legal bases for processing (including consent and legitimate interests), and data subject rights (including access, rectification, erasure, and data portability).

Article 31 of the draft Law governs transfers of personal data out of the Kingdom of Cambodia. Such transfers are permitted if the data controller ensures that the recipient provides a level of personal data protection equivalent to or higher than the level established by the Law.

The Article clarifies that controllers remain accountable for personal data under their control even after it is transferred out of the Kingdom of Cambodia and must take appropriate measures to ensure continuous protection of the personal data. It also empowers the MPTC to **suspend or prohibit** CBDTs if it determines that the transfer poses a serious risk to the rights and freedoms of data subjects or violates the provisions of the Law.

Further details regarding the conditions, formalities, and procedures for personal data transfer outside Cambodia are expected to be determined in forthcoming "Common Guidelines for Personal Data Protection," which will be developed by the MPTC under Article 32 of the draft Law.

Indonesia

1. Personal Data Protection Law

Indonesia's **Personal Data Protection Law** (**PDPL**) became fully enforceable on 17 October 2024, following a two-year transitional period.

As detailed in FPF's 2023 Issue Brief, **Article 56** of the PDPL establishes a hierarchical approach to ensure adequate protection during cross-border transfers:

- **Equivalent or Higher Level of Protection**: Controllers must first ensure that the jurisdiction where the recipient of personal data is located provides a level of personal data protection that is equivalent to, or higher than, that under the PDPL.
- **Adequate and Binding Protection**: If the first condition cannot be met, the controller must then ensure that there is "adequate and binding personal data protection" in place. The PDPL does not expand on the scope of this term.
- **Data Subject's Consent**: If neither of the previous two conditions can be satisfied, the controller must obtain explicit consent from the data subject for the transfer.

However, Article 56 of the PDPL leaves much of the implementing detail for these provisions to implementing regulations, which have only recently been enacted.

2. Draft Implementing Regulations for the PDPL

On 16 July 2026, the Government of Indonesia enacted and promulgated **Government Regulation No. 33 of 2026 on the Implementation of Law No. 27 of 2022 on Personal Data Protection** (**Regulation**). The Regulation will take effect six months after its promulgation (i.e., 16 January 2027).

Chapter V (Articles 160 to 174) of the Regulations expand on the PDPL's CBDT requirements.

Assessment of Equivalent or Higher Protection

Article 168 of the Regulation provides that Indonesia's DPA (once established) will be responsible for assessing whether jurisdictions or international organizations offer an equivalent or higher level of personal data protection to the PDPL.

This assessment evaluates countries based on three criteria: (1) legal regulations for personal data protection; (2) the existence of a supervisory institution or authority for personal data protection; and (3) any international commitments or legally binding obligations related to personal data protection.

Forms of Adequate and Binding Protection

Article 169 of the Regulation provides that "adequate and binding personal data protection" for purposes of Article 56 of the PDPL may take the form of any of the following:

- **Binding bilateral, multilateral, or regional agreements** relating to personal data transfers that can be enforced by both agencies and authorities;
- **SCCs:** Article 170 of the Regulation indicates that the SCCs will be designated by Indonesia's DPA. The SCCs will minimally cover the legal basis for processing, data protection clauses, notification obligations for data protection failures, and due diligence requirements for other data recipients. Controllers will be able to add further provisions and have the option to consult with Indonesia's DPA on this.
- **BCRs:** Article 170 of the Regulation indicates that BCRs must be approved by the DPA. They must specify the receiving party's obligation to provide equivalent or higher data protection than the PDPL, the bound parties, designate countries and territories for data transfer, and the division of roles, rights, and obligations among involved parties
- **Other instruments** recognized by Indonesia's DPA.

Controllers are required to document their compliance with these measures in written and/or recorded form.

The draft regulations also note that transfers ordered by foreign courts, tribunals, or administrative authorities are only recognized if underpinned by an international agreement.

Consent for CBDTs

Article 173 of the Regulation introduces additional requirements for consent-based data transfers, on top of those in the PDPL. Specifically,

- The transfer must:
    - be “non recurring” – this phrase is not explained but likely means that the data transfer should be a one-off event, rather than a continuous or regular process;
    - involve a limited number of data subjects; and
    - be necessary for purposes that do not override the data subject's rights and freedoms.
- The controller must also assess the risks from the transfer and implement appropriate protective measures.
- The controller must also inform both Indonesia's DPA and the data subject about the transfer and the urgent legitimate interests that are fulfilled by such transfer.

Additional Obligations During Transfer

Articles 161 to 164 of the Regulations provides a detailed list of additional obligations for controllers and processors involved in CBDTs. These include:

- **Recording and mapping** the data transfer cycle and its implications.
- Ensuring that the transferred data is **sufficient, relevant, and limited to the transfer's purpose**.
- Prior to the transfer,
    - **Assessing the effectiveness of legal instruments** to be used based on criteria in Article 162, considering the use of supplementary instruments (contractual, technical, and/or organizational) if necessary, and periodically re-evaluating the transfer mechanisms to ensure continued effectiveness;
    - **Conducting an impact assessment** considering the risks to data subjects’ rights; and
    - Notifying the data subject of the purpose, existing protection instruments, mechanisms for protecting data subject rights, risks, and mitigation measures.
    - An exception applies for transfers protecting the vital interests of the data subject, where information can be provided after the transfer.

Administrative Sanctions

Violations of the Regulation's cross-border data transfer provisions are subject to administrative sanctions under Article 184, which may include:

- Written warnings.
- Temporary suspension of personal data processing activities.
- Deletion or destruction of personal data.
- Administrative fines, of up to 2% of the annual income or revenue of the controller or processor, calculated based on factors such as the impact and duration of the violation, types of data affected, number of individuals impacted, and the controller's cooperation during investigation (see Article 185).

Malaysia

Since 2023, Malaysia's CBDT framework has undergone significant developments, transitioning from a non-operational whitelist system to a controller-led assessment model for cross-border data transfers. This new model requires data controllers to perform a TIA to ensure destination jurisdictions offer "substantially similar" or "equivalent" data protection. It also formalizes specific safeguards like BCRs, contractual clauses, and certifications to facilitate these transfers.

1. Personal Data Protection (Amendment) Act 2024

The Personal Data Protection (Amendment) Act 2024 (**Amendment Act**), which was enacted on 17 October 2024 and took full effect on 1 April 2025, introduced significant changes to Malaysia's CBDT framework, replacing an unimplemented "whitelist" mechanism with a new mechanism allowing controllers to assess whether a third jurisdiction provides a level of protection that is either **"substantially similar"** or **"equivalent" to Malaysia's** Personal Data Protection Act 2010 (**PDPA**).

Prior to these amendments, Section 129(1) of the PDPA provided a mechanism allowing transfers to jurisdictions that had been whitelisted by Malaysia's Government. However, this provision was never implemented, and no jurisdictions were ever whitelisted.

The amendments replaced the unimplemented whitelist with a new provision allowing controllers to transfer personal data to jurisdictions that either:

- Have laws that are substantially similar to the PDPA; or
- Ensure an equivalent level of protection to the PDPA.

The Amendment Act did not change any of the other existing mechanisms for transferring personal data out of Malaysia, such as consent, implementing safeguards, and necessity for various important purposes.

2. New Guideline on CBDTs

On 29 April 2025, Malaysia's Personal Data Protection Department (**PDPD**) issued a new guideline on CBDTs (**Guideline**) that clarified the requirements for transferring personal data out of Malaysia under both existing mechanisms and the new "substantially similar or equivalent protection" mechanism introduced in the 2024 amendments to the PDPA.

Introduction of TIAs for the New "Substantially Similar or Equivalent Protection" Mechanism

In order to rely on the new "substantially similar or equivalent protection" mechanism, controllers must conduct a TIA, which is valid for three years. The Guideline lists several factors to consider in the TIA, depending on whether the transfer is: (1) to a jurisdiction with substantially similar laws to the PDPA; or (2) subject to equivalent levels of protection to those in the PDPA.

- To determine whether a third jurisdiction's law is "**substantially similar**" to the PDPA, the TIA must assess whether:
    - The law provides:
        - Similar data subject rights;
        - Similar Personal Data Protection Principles;
        - Similar requirements for processing, including collection, disclosure, retention, and cross-border transfers;
        - Similar requirements concerning Data Protection Officers (**DPOs**);
        - Similar data breach notification requirements;
        - Similar requirements imposed on data processors to protect personal data; and
    - There exists a regulatory authority that is similar to the PDPD and has effective enforcement powers.
- To determine whether a transfer is subject to an "**equivalent level of protection**" to that in the PDPA, the TIA may also consider if the recipient of the personal data has:
    - Security measures and policies aligned with the Security Principle under the PDPA and the Personal Data Protection Standard;
    - Security-related certifications;
    - Legally enforceable obligations (contract, agreement, or law) enforceable by the data controller or data subject;

- An easily enforceable relevant personal data protection law;
- A good history of compliance and no significant data breach incidents;
- Requirements imposed on data processors to protect personal data; and
- A regulatory authority similar to the PDPD that performs data protection functions

The Guideline indicates which **sources of information** a controller may rely on when conducting a TIA. These include laws, regulations, guidelines, case law, reports from intergovernmental organizations, news reports of data breaches, and reports from the receiver itself.

The Guideline also specifies that if there are changes or amendments to the relevant personal data protection laws, or to systems or policies related to data security, during the validity period of the TIA, the controller must review these changes to determine if the law remains substantially similar to the PDPA.

Safeguards

The Guideline also outlines appropriate safeguards that data controllers may rely on to comply with Section 129(3)(f) of the PDPA, which permits transfers of personal data out of Malaysia if the controller has taken all reasonable precautions and exercised all due diligence to ensure that post-transfer, the personal data will not be processed in contravention of the PDPA.

These safeguards include:

- **BCRs**;
- **Contractual clauses** – the Guideline specifically references the ASEAN MCCs and EU's SCCs; and
- **Certification under a suitable scheme**, such as Europrivacy, the UK Legal Services Operational Privacy Certification Scheme, or the APEC CBPR or PRP schemes, among others.

3. Membership in the APEC CBPR System

On 3 November 2026, Malaysia's Personal Data Protection Commissioner announced, via the PDPD's LinkedIn page, that Malaysia had officially been accepted as a full member of the APEC CBPR System, following the 2024 amendments to the PDPA (see above). This announcement complements the PDPD's April 2025 CBDT Guideline, which recognizes the APEC CBPR scheme as an appropriate safeguard under Section 129(3)(f) of the PDPA. The Ministry of Digital also indicated that it is currently exploring a proposal to expand Malaysia's participation to the Global CBPR Forum as well.

Singapore

In March 2026, amendments to Regulation 12 of Singapore's Personal Data Protection Regulations (PDPR) came into effect. This Regulation outlines international privacy certifications that are recognized as valid legal bases for transferring personal data out of Singapore, in line with Regulation 10 of the PDPR and Section 26 of Singapore's Personal Data Protection Act.

Prior to the amendment, Regulation 12 of the PDPR recognized the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems. The amendments add the Global CBPR and Global PRP systems to this list.

Thailand

1. CBDT Regulations

Thailand's Personal Data Protection Act (**PDPA**) provides two main mechanisms for transferring personal data abroad: Section 28 (Adequacy) and Section 29 (Safeguards). On 25 December 2023, Thailand's Personal Data Protection Committee (**PDPC**) released two regulations which implement each of these mechanisms.

Section 28 Regulation – "Adequacy" Mechanism

Section 28 of the PDPA allows personal data to be transferred to a foreign country or international organization that has an adequate standard of data protection (among other mechanisms).

The regulation on Section 28 of the PDPA clarifies that the PDPC is responsible for assessing whether a destination country or international organization provides an adequate level of data protection and may establish a list of destination countries or international organizations that meet this requirement.

In doing so, the PDPC will consider the following factors:

- The presence of legal measures and mechanisms consistent with Thailand's PDPA, ensuring appropriate and enforceable personal data protection measures, data subject rights, and effective legal remedies.

- The existence of an agency with duties and powers to enforce data protection laws in the destination country or organization.

The regulation also provides that controllers can submit concerns about a destination's adequacy for adjudication by the PDPC.

Section 29 Regulation – "Safeguards" Mechanism

Section 29 of the PDPA applies when a destination country or international organization does not have adequate data protection standards under Section 28, or if another mechanism under Section 28 (such as consent or necessity) is not applicable.

In such cases, the controller or processor must implement "appropriate safeguards." According to the regulation on Section 29 of the PDPA, these include:

- **BCRs for Intragroup Transfers:** Organizations transferring data within the same business group must submit a "Personal Data Protection Policy" to the PDPC for examination and certification. This policy must be legally valid and enforceable within the group, and provide for the protection of data subject rights, complaint mechanisms, and security measures consistent with minimum legal standards.

- **Other Safeguards for Transfers to External Parties:**

    - **Contractual Terms:** These explicitly define duties, roles, and responsibilities for data protection, including: collection, use, and disclosure of personal data; security measures consistent with Thai standards; processing only at the sender's instruction and purpose; cooperation on upholding data subject rights; data retention and deletion; and breach notification within 72 hours. They must also ensure effective legal remedies for data subjects. The regulation specifically recognizes the **ASEAN MCCs** and **EU SCCs** as valid contractual terms. It also indicates that the PDPC will publish details of model contracts on its website.

    - **Certification**: Certification regarding personal data processing for cross-border transfers, ensuring appropriate measures meet accepted standards.

    - **Government Agreements**: Legally binding and enforceable agreements between Thai and foreign government agencies.

2. BCR Regulations

On 17 February 2026, the PDPC issued a new Regulation on the Examination and Certification of Binding Corporate Rules within the Same Affiliated Business or the Same Group of Undertakings.

This Regulation further operationalizes Section 29 of the PDPA by establishing procedures for entities incorporated in Thailand to submit BCRs for intergroup transfers of personal data for review and certification by the PDPC.

In order to be certified, the BCRs must be legally binding and enforceable across all participating entities within the corporate group and include mechanisms to ensure and monitor compliance with the PDPA. Once certified, entities may rely on the BCRs to transfer personal data out of Thailand to affiliated entities within the same corporate group.

Vietnam

Since 2023, Vietnam has undertaken a transformative legislative overhaul of its digital landscape, culminating in a new, comprehensive, and state-controlled data governance framework. This framework is built upon three core pillars: (1) the **Law on Personal Data Protection** (**PDP Law**); (2) the **Data Law**; and (3)

the **Law on the Digital Technology Industry** (**DTI Law**). The PDP Law and Data Law in particular significantly impact requirements for transferring personal data out of Vietnam. Readers interested in a deeper dive into Vietnam's PDP Law and the Data Law may refer to FPF's Issue Brief, published in December 2025, here.

1. Law on Personal Data Protection (PDP Law)

The PDP Law was passed by Vietnam's National Assembly on 26 June 2025 and became effective from 1 January 2026. It shares many similarities with the existing Personal Data Protection Decree (**Decree**), enacted in 2023, but as a full-fledged law, occupies a higher position in Vietnam's legislative hierarchy.

Article 20 of the PDP Law provides for CBDTs out of Vietnam. Like the earlier Decree, the PDP Law provides for only a single mechanism for transferring personal data out of Vietnam: a data transferor must prepare a comprehensive **TIA dossier** and submit a copy to the Ministry of Public Security (**MPS**) within 60 days of initiating the data transfer.

However, unlike the Decree, the PDP Law provides exceptions to the TIA requirement, including where:

- Employee data is processed and stored in the cloud.
- Data subjects initiate the transfer of their own personal data out of Vietnam.
- Transfers are conducted by state agencies.

The TIA dossier must be reviewed every 6 months and retained for annual inspection by the Department of Cybersecurity and High-tech Crime Prevention (also known as "**A05**"), a division within the MPS. Considering that the MPS's core mandate is national security and crime prevention, TIA reviews will likely be conducted through a national security lens. Article 20 of the PDP Law also expressly empowers A05 to suspend CBDTs of personal data that may cause harm to Vietnam's national defense and security.

The PDP Law also introduces a much stricter penalty scheme than that under the earlier Decree. Violations of the PDP Law's CBDT requirements are subject to administrative fines of up to 5% of a company's total revenue from the preceding financial year. If there was no revenue, or if 5% is less than VND 3 billion (approximately USD 114,000), the fine is capped at VND 3 billion.

2. Data Law

The Data Law was passed on 30 November 2024 and became effective from 1 July 2025. It is fundamentally a national security instrument and is enforced by the MPS and the Ministry of National Defense. The Data Law also has a far broader scope than the PDP Law, regulating all "digital data" (including personal, non-personal, public, and business data) which it treats as a strategic national asset.

The Data Law introduces new, critical classifications which are subject to CBDT restrictions:

- **"Important Data"** is data that can *potentially* impact national defense, security, foreign affairs, macroeconomics, social stability, and public health and safety. Transfers of Important Data require

a five-day prior notification to the authorities, who retain the power to suspend the transfer if they identify security risks

- **"Core Data"** is a subset of important data that *directly* impacts the same critical national interests. Transfers of Core Data require explicit government approval, following a 10-day review by authorities.

The specific types of data falling into these categories are enumerated in official lists promulgated by the Prime Minister (e.g., Decision 20/2025/QD-TTg, issued on 1 July 2025). These lists are extensive and can be updated more easily than laws, creating a risk of regulatory uncertainty.

Administrators of Important and Core Data are also required to conduct periodic risk assessments of their processing activities and notify the MPS and/or the Ministry of National Defense (biannually for Core Data, annually for Important Data).

3. Decree No. 356/2025/ND-CP

On 31 December 2025, the Government of Vietnam enacted Decree No. 356/2025/ND-CP (Decree 356/2025), which took effect on 1 January 2026. This Decree provides critical implementing details for the PDP Law, specifically clarifying the operational requirements for CBDTs and establishing important exemptions to the TIA regime.

Operationalizing the TIA Regime

Decree 356/2025 clarifies that organizations must submit their TIA dossier to the MPS within **60 days of proceeding with a CBDT**. The dossier requires granular detail, including system diagrams, data flow charts, and an assessment of the recipient's data protection standards.

Organizations must update their TIA dossier **every 6 months** if there are **changes to the processing activity**. However, **significant changes**, such as organizational restructuring or a change in data protection service providers, trigger a strict requirement to update the dossier within **10 days**.

Notably, **Article 17** of Decree 356/2025 explicitly empowers the MPS to order the **suspension** of a CBDT if the data is used for activities that infringe upon national defense or security, or if violations of data protection regulations cause harm to national defense or security.

Exemptions from TIA Requirements

Crucially, **Article 17(3)** of Decree 356/2025 introduces specific exemptions where a TIA dossier is not required. Beyond transfers involving state secrets or pressing public tasks, organizations are exempt from submitting a TIA for:

- Press and media activities;
- Transfers of personal data that has already been lawfully publicized;

- Emergency situations involving the protection of life or health, and the safety of property;
- CBDTs required to manage labor agreements; and
- Performing procedures or signing contracts related to cross-border transportation, logistics, money transfers, payments, hotel bookings, or visa and scholarship applications.

Thresholds and Sensitive Data

Decree 356/2025 also clarifies the scope of the PDP Law's exemption for start-ups and small enterprises. It clarifies the threshold for determining whether an individual or organization processes a "large number of personal data subjects" – which disqualifies an entity from the exemption – as **100,000 individuals**.

Further, the Decree significantly expands the definition of "sensitive personal data" to explicitly include financial data, location data, and data tracking behavior in cyberspace. This expanded definition is critical for compliance, as the processing of sensitive personal data also disqualifies small enterprises from the TIA exemption.

Interoperability with the Data Law

As the PDP Law and the Data Law are both full-fledged laws, they are on equal footing. In situations where the provisions of both Laws apply to the same data transfer, organizations cannot choose to comply with one over the other: they must adhere to the cumulative requirements of both.

Crucially, **Article 42** of Decree 356/2025 amends the implementing decree for the Data Law (Decree 165/2025/ND-CP) to resolve regulatory overlaps. It clarifies that if "Core Data" or "Important Data" under the Data Law also qualify as "personal data" under the PDP Law, then organizations are only required to conduct impact assessments under the PDP Law framework. This effectively removes the burden of conducting duplicate risk assessments under the Data Law for these specific datasets.

4. Draft Data Security Law

Vietnam is also in the process of establishing a third pillar of its data governance framework: The Data Security Law. This Law seeks to establish a risk-based data security regime that would sit alongside the existing Data Law and the PDP Law.

On 23 September 2026, the Government of Vietnam released an initial draft of the Data Security Law (drafted by the MPS) for public consultation (**September 2026 Draft**). Subsequently, in mid-October 2026, the Government reportedly submitted a revised draft of the Law (**October 2026 Draft**) to the National Assembly for consideration and comments. While the text of the September 2026 Draft is publicly available, the October 2026 Draft has not been released to the public to date and remains subject to further revision.

(1) September 2026 Draft

Under **Article 8** of the September 2026 Draft of the Data Security Law, data is classified into four risk tiers (Levels 1 to 4). **Article 17** of the September 2026 Draft establishes a tiered framework for transferring data out of Vietnam across these tiers with specific CBDT obligations applying to Level 3 and Level 4 data. Levels 3 and 4 correspond with “Important” and "Core” Data" as defined in lists promulgated by the Prime Minister under the Data Law.

- Transfers of **Level 3** data would be subject to at least 15 days’ prior notification to the MPS, though prior approval is not required. The MPS is empowered to suspend a transfer in writing for up to 30 days (extendable once for an additional 30 days) if it identifies a serious, evidence-based risk to national security, large-scale data leakage, or a breach of data protection commitments by the recipient.

- Transfers of **Level 4** data would generally be subject to mandatory appraisal (*thẩm định*) and written approval by the MPS before the transfer may proceed. An **exemption** applies for **trade secret data** if: (1) the destination jurisdiction is recognized by the Government as providing an "equivalent" level of data protection; (2) the parties execute Government-issued standard contractual clauses; or (3) the transferring entity holds a data-security conformity certification.

- However, transfers of certain subcategories of **Level 4** data would be **prohibited** unless exceptionally authorized in writing by the Prime Minister to serve especially important national interests in foreign affairs, defense, or pursuant to international commitments. These subcategories include data concerning Vietnam’s borders and territorial sovereignty, military or defence works, protection of critical information infrastructure, and large-scale biometric information.

Notably, **Article 17(2)** of the September 2026 Draft **exempts** The transferring entity must declare the data as a trade secret. It then assumes legal responsibility for that assessment and remains subject to inspection by the MPS.

Article 17(5) of the September 2026 Draft introduces **data residency mandates**.

- **Level 4** data must be stored exclusively on critical national data infrastructure within Vietnam, with no exception for international cloud storage.

- Level 3 data that has a "**direct, immediate impact" on national defense, security, banking and finance, energy, or telecommunications** – based on quantitative criteria to be prescribed by the Government – must also be stored at data centers within Vietnam. However, organizations may store such Level 3 data on international cloud infrastructure if they maintain a local backup in Vietnam that state authorities can access and inspect when necessary.

  For the most sensitive subset of this data (i.e., data directly serving defense and security, or posing immediate systemic risks to banking and finance, energy, or telecommunications at a national scale), the local backup must be maintained in real time.

To mitigate regulatory overlap across Vietnam's data governance laws, **Articles 10(3)**, **17(6)**, and **24** of the September 2026 Draft consolidate compliance procedures. Where a cross-border transfer involves data that qualifies both as "personal data" under the PDP Law and as Level 3 or Level 4 data, organizations are only required to complete a single consolidated impact assessment and transfer procedure under the Data Security Law. Transfers of personal data that do not fall within Level 3 or Level 4 remain governed solely by the TIA regime under the PDP Law (see above).

Violations of the September 2026 Draft carry significant **penalties**.

- Under **Article 17(6)**, foreign enterprises that breach Article 17 and fail to remedy the violation following a written warning may be ordered by the MPS to establish local infrastructure and store data in Vietnam, or face technical blocking measures for up to 6 months (extendable once for an additional 6 months).

- Under **Article 23(9)**, serious administrative violations involving Level 3 or Level 4 data are subject to fines of **up to 5% of the offending organization's annual revenue in Vietnam** from the preceding financial year.

- For **multinational corporations**, this cap increases to **5% of global consolidated revenue** if the group's Vietnam revenue is less than 5% of its global revenue, or if the impact of the violation extends beyond Vietnam's territory.

Revisions in the Unreleased October 2026 Draft

According to an official press release, the revised October 2026 Draft presented to the National Assembly **expands the risk classification framework from four to five tiers**, with the overseas transfers of Level 5 data explicitly prohibited unless authorized by the Prime Minister.

Third-party reporting on the National Assembly's deliberations suggests that the Vietnamese Government is considering shifting the focus of the October 2026 Draft towards controlling decryption keys rather than mandatory data localization.[2] Lawmakers reviewing the draft reportedly proposed restrictions on transferring decryption keys and cryptographic parameters associated with Level 4 and Level 5 data outside Vietnam. During parliamentary debates, lawmakers also reportedly called for clearer rules distinguishing the inherent classification of data from the specific risks associated with a particular transfer – such as differentiating between transferring unencrypted data overseas for long-term storage and transferring encrypted data for technical processing or "controlled, remote technical access" – to avoid disrupting routine cross-border operations in sectors such as international payments, cloud computing, and centralized technology services.

[2] Hoa Dinh, "Vietnam considers decryption-key controls as alternative to data localization", mlex, October 27, 2026.



Washington, DC | Brussels | Singapore

FPF.org